A Review on Attack and Security Tools at Network Layer of IoT

Vidur Agarwal, Preeti Mishra, Sachin Kumar, and Emmanuel S. Pilli

Abstract Internet of things (IoT) is one of the emerging areas which connects billions of the devices across the world through Internet. Security and privacy in such a technological era is one of the major challenges. The IoT devices are vulnerable to dangerous attacks at various layers such as application layer, network layer, and perception layer because of their simple architecture and less secure network. In this paper, we mainly focus on the network layer security of IoT. We provide a detailed taxonomy of various attack and security tools at the network layer of IoT. We also provide a comparative analysis of these tools. We hope that our work will be helpful to the researchers working in the area of IoT security to gain better understanding about various existing tools.

Keywords Security and privacy · Attack tools · Security tools

1 Introduction

The worldwide expansion of the Internet and its availability to more than 4 billion end users has given exponential rise to the Internet of things (IoT) [1]. The IoT has made the lives of people more comfortable and easy, leading to reduced human intervention. These smart things connected to the Internet has simplified almost all the important aspects of daily necessity such as connected car, smart refrigerator, IP cameras, and healthcare systems. Since the last decade, almost half of the population of the world is using the Internet because of the advantages provided by it. The IoT devices are vulnerable to attacks because of their simple architecture and less secure network. To perform various attacks, there exits attack tools such as Aircrack-ng [2],

V. Agarwal (✉) · S. Kumar
Graphic Era Deemed to be University, Dehradun, India

P. Mishra
Doon University, Dehradun, India

E. S. Pilli
Malaviya National Institute of Technology, Jaipur, India

M. Tiwari et al. (eds.), *Optical and Wireless Technologies*, Lecture Notes in Electrical Engineering 771, https://doi.org/10.1007/978-981-16-2818-4_54